SLOVENSKI STANDARD
SIST-TS CEN ISO/TS 24534-4:2008

01-junij-2008

Avtomatiļ na identifikacija vozil in opreme - Elektronska identifikacija registracije (ERI) za vozila - 4. del: Varne komunikacije, pri katerih se uporabljajo asimetriļ ne tehnike (ISO/TS 24534-4:2008)

Automatic vehicle and equipment identification - Electronic Registration Identification (ERI) for vehicles - Part 4: Secure communications using asymmetrical techniques (ISO/TS 24534-4:2008)

Straßenverkehrstelematik (RTTT) - Automatische Identifizierung von Fahrzeugen und Ausrüstungen - Elektronische Identifizierung für die Registrierung (ERI) - Teil 4: Sichere Anwendungsebene mittels asymmetrischer Techniken (ISO/TS 24534-4:2008)

Identification automatique des véhicules et des équipements - Identification d'enregistrement électronique (ERI) pour les véhicules - Partie 4: Communications sûres utilisant des techniques asymétriques (ISO/TS 24534-4:2008)

Ta slovenski standard je istoveten z: **CEN ISO/TS 24534-4:2008**

ICS:

03.220.20	Cestni transport	Road transport
35.240.60	Uporabniške rešitve IT v transportu in trgovini	IT applications in transport and trade

SIST-TS CEN ISO/TS 24534-4:2008 **en**

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN ISO/TS 24534-4

February 2008

ICS 35.240.60; 03.220.20

English Version

Automatic vehicle and equipment identification - Electronic Registration Identification (ERI) for vehicles - Part 4: Secure communications using asymmetrical techniques (ISO/TS 24534-4:2008)

Identification automatique des véhicules et des équipements - Identification d'enregistrement électronique (ERI) pour les véhicules - Partie 4: Communications sûres utilisant des techniques asymétriques (ISO/TS 24534-4:2008)

Straßenverkehrstelematik (RTTT) - Automatische Identifizierung von Fahrzeugen und Ausrüstungen - Elektronische Identifizierung für die Registrierung (ERI) - Teil 4: Sichere Anwendungsebene mittels asymmetrischer Techniken (ISO/TS 24534-4:2008)

This Technical Specification (CEN/TS) was approved by CEN on 17 July 2006 for provisional application.

The period of validity of this CEN/TS is limited initially to three years. After two years the members of CEN will be requested to submit their comments, particularly on the question whether the CEN/TS can be converted into a European Standard.

CEN members are required to announce the existence of this CEN/TS in the same way as for an EN and to make the CEN/TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the CEN/TS) until the final decision about the possible conversion of the CEN/TS into an EN is reached.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: rue de Stassart, 36 B-1050 Brussels

Contents

Page

Foreword

This document (CEN ISO/TS 24534-4:2008) has been prepared by Technical Committee CEN/TC 278 "Road transport and traffic telematics", the secretariat of which is held by NEN, in collaboration with Technical Committee ISO/TC 204 "Transport information and control systems".

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

According to the CEN/CENELEC Internal Regulations, the national standards organizations of the following countries are bound to announce this CEN Technical Specification: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

TECHNICAL SPECIFICATION

ISO/TS 24534-4

First edition
2008-02-15

Automatic vehicle and equipment identification — Electronic Registration Identification (ERI) for vehicles —

Part 4: Secure communications using asymmetrical techniques

Identification automatique des véhicules et des équipements — Identification d'enregistrement électronique (ERI) pour les véhicules —

Partie 4: Communications sûres utilisant des techniques asymétriques

Reference number
ISO/TS 24534-4:2008(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

In other circumstances, particularly when there is an urgent market requirement for such documents, a technical committee may decide to publish other types of normative document:

— an ISO Publicly Available Specification (ISO/PAS) represents an agreement between technical experts in an ISO working group and is accepted for publication if it is approved by more than 50 % of the members of the parent committee casting a vote;

— an ISO Technical Specification (ISO/TS) represents an agreement between the members of a technical committee and is accepted for publication if it is approved by 2/3 of the members of the committee casting a vote.

An ISO/PAS or ISO/TS is reviewed after three years in order to decide whether it will be confirmed for a further three years, revised to become an International Standard, or withdrawn. If the ISO/PAS or ISO/TS is confirmed, it is reviewed again after a further three years, at which time it must either be transformed into an International Standard or be withdrawn.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/TS 24534-4 was prepared by Technical Committee ISO/TC 204, *Intelligent transport systems*, and by Technical Committee CEN/TC 278, *Road transport and traffic telematics* in collaboration.

ISO/TS 24534 consists of the following parts, under the general title *Automatic vehicle and equipment identification — Electronic Registration Identification (ERI) for vehicles*:

— *Part 1: Architecture*

— *Part 2: Operational requirements*

— *Part 3: Vehicle data*

— *Part 4: Secure communications using asymmetrical techniques*

— *Part 5: Secure communications using symmetrical techniques*

Introduction

A quickly emerging need has been identified within administrations to improve the unique identification of vehicles for a variety of services. Situations are already occurring where manufacturers intend to fit lifetime tags to vehicles. Various governments are considering the needs/benefits of ERI such as legal proof of vehicle identity with potential mandatory usages. There is a commercial and economic justification both in respect of tags and infrastructure that a standard enables an interoperable solution.

Electronic Registration Identification (ERI) is a means of uniquely identifying road vehicles. The application of ERI will offer significant benefits over existing techniques for vehicle identification. It will be an enabling technology for the future management and administration of traffic and transport, including applications in free-flow, multi-lane, traffic conditions with the capability to support mobile transactions. ERI addresses the need of authorities and other users for a trusted electronic identification, including roaming vehicles.

This part of ISO/TS 24534 specifies the application layer interfaces for the exchange of data between an onboard component containing the ERI data and a reader or writer inside or outside the vehicle.

The exchanged identification data consists of a unique vehicle identifier and may also include data typically found in the vehicle's registration certificate. The authenticity of the exchanged vehicle data can be further enhanced by ensuring data has been obtained by request from a commissioned device, with the data electronically signed by the registration authority.

In order to facilitate (international) re-sales of vehicles, the ERI interface includes provisions for another accredited registration authority to take over the registration of a vehicle.

The ERI interface supports confidentiality measures to adhere to (inter)national privacy regulation and to prevent other misuse of electronic identification of vehicles. A registration authority may authorize other authorities to access the vehicle's data. A holder of a registration certificate may authorize an additional service provider to identify the vehicle when he/she wants commercial service.

However, it is perceived that different users may have different requirements for authentication and confidentiality. This Technical Specification therefore supports different levels of security with maximum compatibility. Much attention is given to the interoperability of the component containing the ERI data and readers of various levels of capability, e.g. the identification of a vehicle with a less capable ERI data component by a more sophisticated reader equipment and vice versa.

The supported complexity of the device containing the ERI data may range from a very simple read-only device that only contains the vehicle's identifier, to a sophisticated device that includes both authentication and confidentiality measures and maintains a historic list of the vehicle data written by the manufacturer and by vehicle registration authorities.

Following the events of 11 September 2001, and subsequent reviews of anti-terrorism measures, the need for ERI has been identified as a possible anti-terrorism measure. The need for International or pan-European harmonization of such ERI is therefore important. It is also important to ensure that any ERI measures contain protection against misuse by terrorists.

This part of ISO/TS 24534 makes use of the basic automatic vehicle identification (AVI) provisions already defined in ISO 14814 and 14816.

Automatic vehicle and equipment identification — Electronic Registration Identification (ERI) for vehicles —

Part 4: Secure communications using asymmetrical techniques

1 Scope

This part of ISO/TS 24534 provides the requirements for an Electronic Registration Identification (ERI) that is based on an identifier assigned to a vehicle (e.g. for recognition by national authorities) suitable to be used for:

- electronic identification of local and foreign vehicles by national authorities,
- vehicle manufacturing, in-life-maintenance and end-of-life identification (vehicle life cycle management),
- adaptation of vehicle data, e.g. in case of international re-sales,
- safety-related purposes,
- crime reduction, and
- commercial services.

It adheres to privacy and data protection regulations.

This part of ISO/TS 24534 specifies the interfaces for a secure exchange of data between an ERT and an ERI reader or ERI writer in or outside the vehicle using asymmetric encryption techniques.

NOTE 1 The onboard device containing the ERI data is called the Electronic Registration Tag (ERT).

This Technical Specification includes:

- the application layer interface between an ERT and an onboard ERI reader or writer,
- the application layer interface between the onboard ERI equipment and external ERI readers and writers, and
- security issues related to the communication with the ERT.

NOTE 2 The vehicle identifiers and possible additional vehicle data (as typically contained in vehicle registration certificates) are defined in ISO/TS 24534-3.

NOTE 3 The secure application layer interfaces for the exchange of ERI data with an ERI reader or writer are specified in ISO/TS 24534-4 and a future ISO/TS 24534-5.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 7498-1:1994, *Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model*

ISO/IEC 7498-2:1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*

ISO/IEC 8824 (all parts), *Information technology — Abstract Syntax Notation One (ASN.1)*

ISO/IEC 8825-2, *Information technology — ASN.1 encoding rules: Specification of Packed Encoding Rules (PER) — Part 2*

ISO/IEC 9798-1:1997, *Information technology — Security techniques — Entity authentication — Part 1: General*

ISO/IEC 10118-1:2000, *Information technology — Security techniques — Hash-functions — Part 1: General*

ISO/IEC 10181-2:1996, *Information technology — Open Systems Interconnection — Security framework for open systems: Authentication framework*

ISO/IEC 10646:2003, *Information technology — Universal Multiple-Octet Coded Character Set (UCS)*

ISO/IEC 14443 (all parts), *Identification cards — Contactless integrated circuit(s) cards — Proximity cards*

ISO/CD 14814, *Road transport and traffic telematics — Automatic vehicle and equipment identification — Reference architecture and terminology*

ISO 14816, *Road transport and traffic telematics — Automatic vehicle and equipment identification — Numbering and data structure*

ISO 15628, *Transport Information and Control Systems (TICS) — Dedicated Short Range Communication (DSRC) — DSRC application layer*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
access control
prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner

[ISO 7498-2, definition 3.3.1]

3.2
access control list
list of entities, together with their access rights, which are authorized to have access to a resource

[ISO 7498-2, definition 3.3.2]

3.3
active threat
threat of a deliberate unauthorized change to the state of the system

[ISO 7498-2, definition 3.3.4]

EXAMPLE Examples of security-relevant active threats may include modification of messages, replay of messages, and insertion of spurious messages, masquerading as an authorized entity and denial of service.

3.4
additional vehicle data
ERI data in addition to the vehicle identifier

[ISO 24534-3, definition 3.1]

3.5
air Interface
conductor-free medium between onboard equipment (OBE) and the reader/interrogator through which the linking of the OBE to the reader /interrogator is achieved by means of electro-magnetic signals

[ISO 14814, definition 3.2]

3.6
authority
organisation that is allowed by public law to identify a vehicle using ERI

3.7
authorization
granting of rights, which includes the granting of access based on access rights

[ISO 7498-2, definition 3.3.10]

3.8
certification authority
natural or legal person trusted to create **public key certificates**

NOTE See also **top-level certification authority** and **intermediate certification authority**.

3.9
challenge
data item chosen at random and sent by the **verifier** to the **claimant**, which is used by the claimant, in conjunction with secret information held by the claimant, to generate a response which is sent to the verifier

[ISO 9798-1, definition 3.3.5]

NOTE In this Technical specification the term challenge is also used in case an ERT does not have enabled encryption capabilities and the challenge is merely copied without any secret information applied.

3.10
ciphertext
data produced, through the use of **encipherment**; the semantic content of the resulting data is not available

[ISO 7498-2, definition 3.3.14]

3.11
claimant
entity which is or represents a principal for the purposes of authentication

NOTE A claimant includes the functions necessary for engaging in authentication exchanges on behalf of a principal.

[ISO 10181-2, definition 3.10]

3.12
cleartext
intelligible data, the semantic content of which is available

[ISO 7498-2, definition 3.3.15]